The equality problem for rational series with multiplicities in the tropical semiring is undecidable

Daniel Krob

The equality problem for rational series with multiplicities in the tropical semiring is undecidable

Daniel KROB

LACIM and CNRS(Institut Blaise Pascal; LITP) [1]

0 Introduction

The tropical semiring is the semiring denoted by $\mathcal{M}$ which has support $\mathbb{N} \cup \{+\infty\}$ and operations $a \oplus b = \min\{a, b\}$ and $a \otimes b = a + b$. It was first introduced in the context of cost minimization in Operations Research. However it appeared that $\mathcal{M}$ plays in fact a central role in several decision problems concerning rational languages (see [8] for a survey of the tropical semiring theory and of its applications). For instance, I. Simon showed that the finite power property for recognizable languages can be reduced to the limitedness problem for the tropical semiring (cf [8]).

One of the main open questions in the theory of the tropical semiring was to see if it is possible to decide whether two given $\mathcal{M}$-rational series are equal or not (cf [8, 9]). We offer here an answer to this problem since we show in this paper that the equality problem for $\mathcal{M}$-rational series over an alphabet with at least two letters is *undecidable*. One should notice that most people thought that a decision procedure existed (cf [8] for instance) and our result is indeed based on a rather surprising encoding of a 10th Hilbert problem.

It is also interesting to precise the structure of the proof of our undecidability result. Indeed it appears that we use as a main tool the tropical "ring" $\mathcal{Z} = (\mathbb{Z} \cup \{+\infty\}, \min, +)$ which is just the extension of $\mathcal{M}$ to arbitrary integers. The importance of $\mathcal{Z}$ comes from the equivalence with respect to decidability of the equality problems for $\mathcal{M}$ and $\mathcal{Z}$. According to this result, we can reduce our problem to showing that the equality problem for $\mathcal{Z}$-rational series over an alphabet with at least two letters is undecidable. To prove this last result, we show in fact that the decidability of the equality problem for $\mathcal{Z}$ is

[1] Mailing adress : Université de Rouen; Faculté des Sciences (Informatique); 76134 Mont Saint-Aignan Cedex - FRANCE

equivalent to the decidability of the local inequality problem for $\mathcal{Z}$. Using this equivalence and a reduction to a 10th Hilbert problem, we prove then the undecidability of the equality problem for $\mathcal{Z}$-rational series over an alphabet with at least two letters. Hence this allows us to obtain the undecidability of the same problem for $\mathcal{M}$-rational series. Moreover our methods give us also immediately other decidability and undecidability results for connected problems. In particular, we solve also another open question (cf [9]) by showing that the equality problem for rational series over an alphabet with at least two letters and with multiplicities in the semiring $\mathcal{N} = (\mathbb{N} \cup \{-\infty\}, \max, +)$ is undecidable.

1 Preliminaries

The *tropical "ring"* is the commutative semiring denoted by $\mathcal{Z}$ which has $\mathbb{Z} \cup \{+\infty\}$ as support, whose addition $\oplus$ is defined by $a \oplus b = \min\{a, b\}$ and whose product $\otimes$ is given by $a \otimes b = a + b$. The operations of $\mathbb{Z}$ are extended to $\mathcal{Z}$ in the usual natural way and the units for $\oplus$ and $\otimes$ are respectively $+\infty$ and 0. The *tropical semiring* is the subsemiring of $\mathcal{Z}$ denoted by $\mathcal{M}$ which has $\mathbb{N} \cup \{+\infty\}$ as support. Let us also introduce the "dual" semiring $\mathcal{N}$ of $\mathcal{M}$ which is the semiring whose support is $\mathbb{N} \cup \{-\infty\}$, whose addition $\oplus$ is given by $a \oplus b = \max\{a, b\}$ and whose product $\otimes$ is defined by $a \otimes b = a + b$. Finally let us consider the subsemiring $\mathcal{Z}^-$ of $\mathcal{Z}$ whose support is $\mathbb{Z}^- \cup \{+\infty\}$. Note that $\mathcal{Z}^-$ is clearly isomorphic to $\mathcal{N}$, an effective isomorphism beeing obtained by the mapping $x \to -x$ from $\mathcal{Z}^-$ into $\mathcal{N}$.

We refer to [2] for all generalities concerning series and rational series with multiplicities in an arbitrary semiring K. We will denote here by $K << A >>$ the K-algebra of series over A with multiplicities in K and by $K\mathrm{Rat}(A)$ the K-algebra of K-rational series. Let us also recall that a K-representation of order n of a free monoid A^* is just a monoid morphism from A^* into the monoid of square matrices of order n with entries in K. Then a K-automaton of order n is a triple (I, μ, T) where μ is a K-representation of order n of A^* and where I and T are respectively a row and a column vector of order n with entries in K (see [2] for more details).

Let us now precise some notions concerning K-rational series that we will use in the sequel. First we will denote by $\underline{L}$ the characteristic series of any language $L \subset A^*$ which is the series of $K << A >>$ defined by

$$\forall\ w \in A^*,\ (\underline{L}|w) = \begin{cases} 1_K & \text{if } w \in L \\ 0_K & \text{if } w \notin L \end{cases}$$

Note that $\underline{L}$ is always a K-rational series when L is a rational language (cf [2]). We also denote here as usually by $S \odot T$ the Hadamard product of two series S, T which is the series defined by $(S \odot T|w) = (S|w)(T|w)$ for every $w \in A^*$. We recall that $S \odot T$ is a K-rational series when S and T are K-rational series (see [2] for more details). Finally the constant K-rational series whose every coefficient is equal to k, will be always denoted by k.

Let us now recall the following result which is folklore (it is in fact a general property of positive semirings).

PROPOSITION 1.1 : Let S be a rational series of $\mathcal{Z}\mathrm{Rat}(A)$. Then the set

$$\{\ w \in A^*,\ (S|w) = +\infty\ \}$$

is a constructible rational language of $\mathrm{Rat}(A)$.

Proof : Let π be the morphism of semirings from $\mathcal{Z}$ into the boolean semiring $\mathcal{B}$ defined by $\pi(+\infty) = 0$ and $\pi(z) = 1$ for every $z \in \mathcal{Z} - \{+\infty\}$. We also denote by π its natural extension as an algebra morphism from $\mathcal{Z} \ll A \gg$ into $\mathcal{B} \ll A \gg$. Then we have

$$\{\ w \in A^*,\ (S|w) = +\infty\ \} = \{\ w \in A^*,\ (\pi(S)|w) = 0\ \}$$

Our result follows now since $\pi(S)$ is clearly a constructible $\mathcal{B}$-recognizable series. ∎

Note : It follows also from proposition 1.1 that it is decidable whether a recognizable series of $\mathcal{Z}\mathrm{Rat}(A)$ is equal to $+\infty$ or whether it has a coefficient equal to $+\infty$.

Finally let us recall the following result of Adler (cf [1, 5]) :

THEOREM 1.2 : Every diophantine equation is equivalent to an equation of the form

$$P(x_1, \ldots, x_n) = 1$$

where P is an homogeneous polynomial of degree 4 of some $\mathbb{Z}$-algebra $\mathbb{Z}[x_1, \ldots, x_n]$.

2 Some relations between decidability problems

Let K be a totally ordered semiring. Let us then consider the four problems of equality, inequality, local inequality and local equality for K-rational series over A :

$$P, Q \in \mathrm{KRat}(A), \quad P = Q \ ? \qquad (Eq)$$

$$P, Q \in \mathrm{KRat}(A), \quad P \leq Q \ ? \qquad (Ineq)$$

$$P, Q \in \mathrm{KRat}(A), \quad \exists\ w \in A^*,\ (P|w) \leq (Q|w) \ ? \qquad (LocalIneq)$$

$$P, Q \in \mathrm{KRat}(A), \quad \exists\ w \in A^*,\ (P|w) = (Q|w) \ ? \qquad (LocalEq)$$

In general, these problems are not connected. [2] However it appears that the three first above problems are equivalent with respect to decidability when K is the tropical "ring" or semiring.

PROPOSITION 2.1 : Let $K = \mathcal{Z}$ or $K = \mathcal{M}$. Then the three following assertions that deal with decidability problems for K-rational series, are equivalent :

1. The equality problem (Eq) is decidable.
2. The inequality problem $(Ineq)$ is decidable.
3. The local inequality problem $(LocalIneq)$ is decidable.

[2] For instance, when $K = \mathbb{N}$, the equality problem is decidable and the inequality problem is undecidable (see [6]).

Proof : The fact that assertion 2 implies assertion 1 is immediate since we have

$$P = Q \iff \left\{ \begin{array}{l} P \leq Q \\ Q \leq P \end{array} \right.$$

The fact that assertion 1 implies assertion 2 follows also immediately from the relation

$$P \leq Q \iff P = P \oplus Q = \min(P, Q)$$

Let us now show that assertion 3 implies assertion 2. Hence let P, Q be two K-rational series where $K = \mathcal{M}$ or $K = \mathcal{Z}$. Then the set $I = \{ w \in A^*, (Q|w) = +\infty \}$ is rational and constructible according to proposition 1.1. Let us now consider the series $\overline{P}$ defined by

$$\overline{P} = (P \odot \underline{A^* - I}) \oplus \underline{I} = \left\{ \begin{array}{ll} 0 & \text{if } w \in I \\ (P|w) & \text{if } w \notin I \end{array} \right.$$

which is clearly K-rational. We can define in the same way the series $\overline{Q}$. Then we have

$$\begin{array}{rcl} P \leq Q & \iff & \overline{P} \leq \overline{Q} \\ & \iff & \forall\ w \in A^*,\ (\overline{P}|w) \leq (\overline{Q}|w) \\ & \iff & \forall\ w \in A^*,\ (\overline{P}|w) < (\overline{Q}|w) + 1 \end{array}$$

this last equivalence coming from the fact that $\overline{Q}$ has no value equal to $+\infty$. It follows immediately from these relations that we have

$$P \leq Q \iff \neg(\exists\ w \in A^*,\ (\overline{P}|w) \geq (\overline{Q} \odot 1|w))$$

Hence it follows clearly from this last equivalence that assertion 3 implies assertion 2.

Let us now show that assertion 2 implies assertion 3. Thus let P, Q be two K-rational series. According to proposition 1.1, the set $I = \{ w \in A^*, (Q|w) = +\infty \}$ is an effective rational language. Hence we can decide if I is empty or not. If I is non-empty, the local inequality problem has obviously a positive answer since every word $w \in I$ satisfies to $(LocalIneq)$. On the other hand, if I is empty, we have

$$\begin{array}{rcl} (LocalIneq) & \iff & \neg(\forall\ w \in A^*,\ (P|w) > (Q|w)) \\ & \iff & \neg(\forall\ w \in A^*,\ (P|w) \geq (Q|w) + 1) \\ & \iff & \neg(P \geq Q \odot 1) \end{array}$$

Note that the second above equivalence follows from the fact that $I = \emptyset$. Hence it follows immediately from these last equivalences that assertion 2 implies assertion 3. This ends the proof of our proposition. ∎

PROPOSITION 2.2 : Let $K = \mathcal{Z}$ or $K = \mathcal{M}$. Then the decidability of the local equality problem $(LocalEq)$ for K-rational series implies the decidability of the local inequality problem $(LocalIneq)$ for K-rational series.

Proof : It is immediate since we clearly have

$$\exists\ w \in A^*,\ (P|w) \leq (Q|w) \iff \exists\ w \in A^*,\ (P|w) = (P \oplus Q|w) = \min((P|w), (Q|w))$$

Hence our proposition is proved. ∎

3 Undecidability of the equality problem for $\mathcal{Z}$

This section is devoted to the proof of the undecidability of the equality problem for $\mathcal{Z}$-rational series over alphabets with at least two letters. This result implies in fact the undecidability of the same problem for $\mathcal{M}$-rational series as we will see later.

THEOREM 3.1 : Let A be any alphabet with at least 2 letters. Then the equality problem is undecidable for $\mathcal{Z}$-rational series over A.

Proof : We should first notice that the decidability of the equality problem for K-rational series on an arbitrary semiring K and over a k-letter alphabet A_k is equivalent to the decidability of the same problem for a l-letter alphabet A_l when $k, l \geq 2$.

Indeed, it suffices to use an adapted encoding of A_k^* over A_l^* in order to prove this result. For instance, let a, b be two letters of A_l and let σ be the monoid morphism from A_k^* into A_l^* defined by $\sigma(a_i) = a^i b$ for every $a_i \in A_k = \{a_1, \ldots, a_k\}$. Then we can also denote by σ its extension as a K-algebra morphism from $K << A_k >>$ into $K << A_l >>$. It is easy to see that σ is injective and preserves rationality. Hence deciding whether two K-rational series E, F of $K << A_k >>$ are equal, is equivalent to deciding whether the two K-rational series $\sigma(E), \sigma(F)$ of $K << A_l >>$ are equal. This proves our claim.

Our undecidability proof is based on a reduction to Adler's restriction of Hilbert's tenth problem (see theorem 1.2). Let now $P(x)$ be an homogeneous polynomial of degree 4 in several indeterminates of $\mathbb{Z}[x]$. [3] By distinguishing all variables, it is easily seen that the equation $P(x) = 1$ can be transformed in an equivalent way as a system of the form :

$$\begin{cases} \sum_{i=1}^{p} p_i \, x_1^{(i)} x_2^{(i)} x_3^{(i)} x_4^{(i)} = 1 \\ \forall \ (i,j,k,l) \in K, \ x_k^{(i)} = x_l^{(j)} \end{cases}$$

where K is some subset of $[1,p] \times [1,p] \times [1,4] \times [1,4]$ and where $(p_i)_{i=1,\ldots,p}$ is a family of integers of $\mathbb{Z}$. But this last system can also be transformed into the single equation

$$- \mid \sum_{i=1}^{p} p_i \, x_1^{(i)} x_2^{(i)} x_3^{(i)} x_4^{(i)} \ - 1 \mid \ - \sum_{(i,j,k,l) \in K} \mid x_k^{(i)} - x_l^{(j)} \mid \ = \ 0 \qquad (HD)$$

Hence, according to Adler's theorem (cf theorem 1.1) and to the undecidability of Hilbert's tenth problem (cf [5]), it follows from our reduction process that it is undecidable to see whether an equation of the form (HD) has a solution in positive integers.

Let now $A = \{a, b, c, d, e\}$ be a five letter alphabet. According to proposition 2.1 and to our first remark, it suffices to show that the local inequality problem for $\mathcal{Z}$-rational series over A is undecidable in order to prove our theorem. We will show this fact by a suitable encoding of equations (HD) in terms of $\mathcal{Z}$-rational series. But let us now give some lemmas that will allow us to construct this encoding.

LEMMA 3.2 : Let $k \in \mathbb{Z}$. Then the series $Coeff(k)$ defined by

[3] Here x denotes of course a vector of variables $x = (x_1, \ldots, x_n)$.

$$(Coeff(k)|w) = \begin{cases} k\, n_1 n_2 n_3 n_4 & \text{if } w = (((a^{n_1}b)^{n_2}c)^{n_3}d)^{n_4} \text{ with } (n_1,n_2,n_3,n_4) \in \mathbb{N}^4 \\ 0 & \text{if } w \notin (((a^*b)^*c)^*d)^* \end{cases}$$

is a $\mathcal{Z}$-rational series of $\mathcal{Z}\mathrm{Rat}(a,b,c,d)$.

Proof : Using the $\mathcal{Z}$-representation μ of order 1 of A^* defined by

$$\mu(a) = (k) \quad \text{and} \quad \forall\ \alpha \in \{b,c,d\},\ \mu(\alpha) = (0)$$

it can easily be shown that the series

$$S(k,a) = \sum_{w \in A^*} k\,|w|_a\ w$$

is $\mathcal{Z}$-rational. Let now L be the rational language $L = (((a^*b)^*c)^*d)^*$. It is then easy to see that $Coeff(k) = (\underline{L} \odot S(k,a)) \oplus \underline{A^* - L}$ which is hence a $\mathcal{Z}$-rational series. ∎

LEMMA 3.3 : Let $k \in [1,4]$ and $\epsilon \in \{-1,+1\}$. Then the series $Var(k,\epsilon)$ defined by

$$(Var(k,\epsilon)|w) = \begin{cases} \epsilon\, n_k & \text{if } w = (((a^{n_1}b)^{n_2}c)^{n_3}d)^{n_4} \text{ with } (n_1,n_2,n_3,n_4) \in \mathbb{N}^4 \\ 0 & \text{if } w \notin (((a^*b)^*c)^*d)^* \end{cases}$$

is a $\mathcal{Z}$-rational series of $\mathcal{Z}\mathrm{Rat}(a,b,c,d)$.

Proof : Suppose first that $k = 4$. Then, arguing as in lemma 3.2, it is easy to see that

$$\sum_{w \in A^*} \epsilon\,|w|_d\ w$$

is a $\mathcal{Z}$-rational series. Hence it can be clearly shown that $Var(4,\epsilon)$ is a $\mathcal{Z}$-rational series by using the same argument than in lemma 3.2.

We will suppose now that $k \in [1,3]$. Then let us denote $a_1 = a, a_2 = b, a_3 = c, a_4 = d$ and let us consider the $\mathcal{Z}$-representation μ of A^* of order 2 defined by $\mu(a_i) = Id_2$ for every $i \notin \{k, k+1\}$ and by

$$\mu(a_k) = \begin{pmatrix} \epsilon & +\infty \\ +\infty & 0 \end{pmatrix} \quad \text{and} \quad \mu(a_{k+1}) = \begin{pmatrix} +\infty & 0 \\ +\infty & 0 \end{pmatrix}$$

The reader will then easily check that we have for every $n \in \mathbb{N}$

$$\mu(a_k^n\, a_{k+1}) = \begin{pmatrix} +\infty & \epsilon\, n \\ +\infty & 0 \end{pmatrix}$$

which is an idempotent matrix. Hence it follows immediately from this last relation that we have for every $(n_1,n_2,n_3,n_4) \in \mathbb{N}^4$

$$(\ 0\ \ +\infty\ )\ \mu(\ (((a^{n_1}b)^{n_2}c)^{n_3}d)^{n_4}\ )\ \begin{pmatrix} +\infty \\ 0 \end{pmatrix} = \epsilon\, n_k$$

Thus, if $S(k,\epsilon)$ denotes the $\mathcal{Z}$-rational series defined by $(S(k,\epsilon)|w) = \mu(w)_{1,2}$ for every $w \in A^*$, we clearly have $Var(k,\epsilon) = (S(k,\epsilon) \odot \underline{L}) \oplus \underline{A^* - L}$ where L denotes the rational language $(((a^*b)^*c)^*d)^*$. It follows immediately that $Var(k,\epsilon)$ is a $\mathcal{Z}$-rational series. This ends the proof of our lemma. ∎

LEMMA 3.4 : Let M be a square matrix of order n and let $p \in \mathbb{N}$. Let us then denote by $E_{n,p}$ and $\mathcal{N}(M,p)$ the square matrices of order $n\,p$ defined by

$$E_{n,p} = \begin{array}{c} \\ n \\ n \\ \vdots \\ n \end{array} \begin{array}{c} \begin{array}{cccc} n & \dots & n & n \end{array} \\ \begin{pmatrix} +\infty & \dots & +\infty & Id_n \\ Id_n & \dots & +\infty & +\infty \\ \vdots & \ddots & \vdots & \vdots \\ +\infty & \dots & Id_n & +\infty \end{pmatrix} \end{array} \quad \text{and} \quad \mathcal{N}(M,p) = \begin{array}{c} \\ n \\ n \\ \vdots \\ n \end{array} \begin{array}{c} \begin{array}{cccc} n & n & \dots & n \end{array} \\ \begin{pmatrix} M & +\infty & \dots & +\infty \\ +\infty & Id_n & \dots & +\infty \\ \vdots & \vdots & \ddots & \vdots \\ +\infty & +\infty & \dots & Id_n \end{pmatrix} \end{array}$$

Let now $(N_i)_{i=1,\dots,p}$ be a family of square matrices of order n. Then we have

$$\mathcal{N}(N_1,p)\,E_{n,p}\,\mathcal{N}(N_2,p)\,E_{n,p}\ \dots\ \mathcal{N}(N_N,p)\,E_{n,p} \ = \ \begin{array}{c} \\ n \\ n \\ \vdots \\ n \end{array} \begin{array}{c} \begin{array}{cccc} n & n & \dots & n \end{array} \\ \begin{pmatrix} N_1 & +\infty & \dots & +\infty \\ +\infty & N_2 & \dots & +\infty \\ \vdots & \vdots & \ddots & \vdots \\ +\infty & +\infty & \dots & N_p \end{pmatrix} \end{array}$$

Proof : It is an easy verification that we leave to the reader. ∎

Let us now consider an equation of the form (HD). Note that we will use in the sequel the notations used in the definition of this equation. Let us then introduce the rational language C over $A = \{a,b,c,d,e\}$ defined by

$$C = (\ (((a^*b)^*c)^*d)^*\,e\ )^p = \ \prod_{i=1}^{p}\ (((a^*b)^*c)^*d)^*\,e$$

Any word w of C can described as follows

$$w = w(\underline{n}) = (((a^{n_1^{(1)}}b)^{n_2^{(1)}}c)^{n_3^{(1)}}d)^{n_4^{(1)}}\ e\ \dots\ (((a^{n_1^{(p)}}b)^{n_2^{(p)}}c)^{n_3^{(p)}}d)^{n_4^{(p)}}\ e$$

where $\underline{n}$ denotes the vector $(n_1^{(1)}, n_2^{(1)}, n_3^{(1)}, n_4^{(1)},\ \dots\ , n_1^{(p)}, n_2^{(p)}, n_3^{(p)}, n_4^{(p)})$ of $\mathbb{N}^{4p}$. Let now (I,μ,T) be an $\mathcal{Z}$-automaton of order n that recognizes the series $Coeff(k)$ of lemma 3.2. Then we can define a $\mathcal{Z}$-representation ν of A^* order $n\,p$ as follows

$$\forall\ \alpha \in \{a,b,c,d\},\ \nu(\alpha) = \mathcal{N}(\nu(\alpha),p) \quad \text{and} \quad \nu(e) = E_{n,p}$$

where we took the notations of lemma 3.4. Then, according to lemma 3.2 and to lemma 3.4, it is easy to see that we have

$$\Big(\ \dots\ +\infty\ \overset{i\downarrow}{I}\ +\infty\ \dots\ \Big)\ \nu(w)\ \begin{pmatrix} \vdots \\ +\infty \\ T \\ +\infty \\ \vdots \end{pmatrix} \overset{i}{\leftarrow} \ = \begin{cases} k\,n_1^{(i)}n_2^{(i)}n_3^{(i)}n_4^{(i)} & \text{if } w = w(\underline{n}) \in C \\ 0 & \text{if } w \notin C \end{cases}$$

where each symbol $+\infty$ denotes in fact a block of order n. Hence it follows immediately that the series $Pol_i(k)$ defined by $(Pol_i(k)|w) = 0$ when $w \notin C$ and by

$$(Pol_i(k)|w) = k\,n_1^{(i)}n_2^{(i)}n_3^{(i)}n_4^{(i)}$$

when $w = w(\underline{n}) \in C$ is a $\mathcal{Z}$-rational series. Hence the series $Pol^+ = Pol_1(p_1) \odot Pol_2(p_2) \odot \dots \odot Pol_n(p_n) \odot -1$ is $\mathcal{Z}$-rational and we clearly have

$$(Pol^+|w) = \begin{cases} \sum_{i=1}^{p} p_i\, n_1^{(i)} n_2^{(i)} n_3^{(i)} n_4^{(i)} \; - 1 & \text{when } w = w(\underline{n}) \in C \\ -1 & \text{when } w \notin C \end{cases}$$

In the same way, the series $Pol^- = Pol_1(-p_1) \odot Pol_2(-p_2) \odot \ldots \odot Pol_n(-p_n) \odot 1$ is $\mathcal{Z}$-rational and we have

$$(Pol^-|w) = \begin{cases} \sum_{i=1}^{p} -\, p_i\, n_1^{(i)} n_2^{(i)} n_3^{(i)} n_4^{(i)} \; + 1 & \text{when } w = w(\underline{n}) \in C \\ 1 & \text{when } w \notin C \end{cases}$$

Hence the series $Pol = Pol^- \oplus Pol^+$ is $\mathcal{Z}$-rational and we clearly have

$$(Pol|w) = -\,|\, \sum_{i=1}^{p} p_i\, n_1^{(i)} n_2^{(i)} n_3^{(i)} n_4^{(i)} \; - 1\,|$$

when $w = w(\underline{n})$ is in C and $(Pol|w) = -1$ when $w \notin C$. Arguing as above, but now with lemma 3.3 instead of lemma 3.2, it is not difficult to see that the series $Var(i,j,k,l)$ defined by $(Var(i,j,k,l)|w) = 0$ when $w \notin C$ and by

$$(Var(i,j,k,l)|w) = -\,|\, n_i^{(k)} - n_j^{(l)}\,| \quad \text{when } w = w(\underline{n}) \in C$$

is $\mathcal{Z}$-rational for every $i, j \in [1,p]$ and $k, l \in [1,4]$. Hence the series HD defined by

$$HD = Pol \;\odot \bigodot_{(i,j,k,l)\in K} Var(i,j,k,l)$$

is a $\mathcal{Z}$-rational series. Moreover it is easily checked that $(HD|w) = -1$ if $w \notin C$ and that

$$(HD|w) = -\,|\, \sum_{i=1}^{p} p_i\, n_1^{(i)} n_2^{(i)} n_3^{(i)} n_4^{(i)} \; - 1\,| \; - \sum_{(i,j,k,l\in K} |\, n_i^{(k)} - n_j^{(l)}\,|$$

when $w = w(\underline{n}) \in C$. It follows then immediately that the diophantine equation (HD) has a solution in positive integers if and only if there exists a word $w \in A^*$ such that $(HD|w) \geq 0$. Hence it follows from a previous remark that the local inequality problem for $\mathcal{Z}$-rational series over A is undecidable. Thus, according to our reduction work, this ends our proof. ∎

Note : Using the same kind of ideas as in the above proof, it can be shown that any diophantine equation of degree k can be encoded as a local inequality problem for $\mathcal{Z}$-rational series over an alphabet with $k+1$-letters.

As an immediate corollary of the previous theorem, we obtain according to propositions 2.1 and 2.2 :

COROLLARY 3.5 : Let A be an alphabet with at least 2 letters. Then the equality, inequality, local equality and local inequality problems are all undecidable questions for $\mathcal{Z}$-rational series over A.

4 Undecidability of the equality problem for $\mathcal{M}$

4.1 Reduction of decidability problems

In this section, we show that the decidability for $\mathcal{M}$ (resp. $\mathcal{N}$) of any problem considered in section 2 is equivalent to the decidability of the same problem for $\mathcal{Z}$. Let us now first prove this equivalence for $\mathcal{M}$ and $\mathcal{Z}$.

THEOREM 4.1 : Let A be an arbitrary alphabet. Then the equality problem, the inequality problem, the local equality problem or the local inequality problem for $\mathcal{M}$-rational series over A is decidable if and only if the same problem is decidable for $\mathcal{Z}$-rational series over A.

Proof : Since all the proofs are the same, we shall only show here the equivalence between the decidability of the equality problems for $\mathcal{M}$ and $\mathcal{Z}$. Clearly we just have then to prove that the decidability of the equality problem in $\mathcal{M}$ implies the decidability of the same problem in $\mathcal{Z}$.

Let then R and S be two $\mathcal{Z}$-rational series over the alphabet A. According to the Kleene-Schützenberger theorem, R and S are $\mathcal{Z}$-recognizable series. Let us now consider two $\mathcal{Z}$-automata (I, μ, T) and (J, ν, F) of order m and n recognizing respectively R and S. Let us then consider for every $k \in \mathbb{Z}$ the new vectors $I(k), J(k), T(k), F(k)$ and the new $\mathcal{Z}$-representations μ_k and ν_k of A^* defined by

$$\forall\ a \in A,\quad \mu_k(a) = (\,\mu(a)_{i,j} + k\,)_{1\le i,j\le m}\ ,\ \nu_k(a) = (\,\nu(a)_{i,j} + k\,)_{1\le i,j\le n}$$

$$I(k) = (\,I_i + k\,)_{i=1,\dots,m}\ ,\ J(k) = (\,J_i + k\,)_{i=1,\dots,n}$$

$$T(k) = (\,T_i + k\,)_{i=1,\dots,m}\ ,\ F(k) = (\,F_i + k\,)_{i=1,\dots,n}$$

It is easy to see that we have

$$I(k)\,\mu_k(w)\,T(k) = I\,\mu(w)\,T + 2k + k|w|$$

$$J(k)\,\nu_k(w)\,F(k) = J\,\nu(w)\,F + 2k + k|w|$$

for every word $w \in A^*$. Let now R_k and S_k be the two series recognized respectively by the automata $(I(k), \mu_k, T(k))$ and $(J(k), \nu_k, F(k))$. It follows immediately from the above computations that we have $S = T$ iff $S_k = T_k$ for any fixed $k \in \mathbb{Z}$. But it is easy to see that T_k and S_k are $\mathcal{M}$-recognizable series when k is greater than

$$-\min_{i,j}\ (\ \mu(a)_{i,j}, \nu(a)_{i,j}, I_i, J_i, T_i, F_i\ )\ \in \mathbb{Z} \cup \{-\infty\}.$$

Hence we showed that the equality of two $\mathcal{Z}$-recognizable series is equivalent to the equality of two $\mathcal{M}$-recognizable series. This ends proving that the decidability of the equality problem for $\mathcal{M}$-rational series implies the decidability of the same problem for $\mathcal{Z}$-rational series. Our theorem is then proved. ∎

Using the same method as in the previous theorem, we can also get the following result that shows our equivalence result for $\mathcal{Z}$ and $\mathcal{N}$.

THEOREM 4.2 : Let A be an arbitrary alphabet. Then the equality problem, the inequality problem, the local equality problem or the local inequality problem

for $\mathcal{N}$-rational series over A is decidable if and only if the same problem is decidable for $\mathcal{Z}$-rational series over A.

Proof : Since all the proofs are similar, we shall also only show here the equivalence between the equality problems for $\mathcal{N}$ and $\mathcal{Z}$. It suffices then clearly to prove that the decidability of the equality problem for $\mathcal{N}$ implies the decidability of the same problem for $\mathcal{Z}$. But since $\mathcal{N}$ is effectively isomorphic to $\mathcal{Z}^-$ (cf section 1), we have just to prove that the decidability of the equality problem for $\mathcal{Z}^-$ implies the decidability of the same problem for $\mathcal{Z}$.

Let us now take the same notations that in the proof of theorem 4.1. It is easy to see that S_k and R_k are $\mathcal{Z}^-$-recognizable series when k is less than

$$M = -\max_{i,j} \left(\mu(a)_{i,j}, \nu(a)_{i,j}, I_i, J_i, T_i, F_i \right) \in \mathbb{Z}$$

where the above maximum is only taken over the values which are not equal to $+\infty$ (when every value involved in the above maximum is equal to $+\infty$, we set $M = +\infty$). Hence, arguing as in the proof of the previous theorem, it follows that the equality of two $\mathcal{Z}$-rational series is equivalent to the equality of two $\mathcal{Z}^-$-rational series. This ends therefore the proof of our theorem. ∎

4.2 Undecidability of the equality problem for $\mathcal{M}$ and $\mathcal{N}$

As immediate corollaries of the previous results, we get the following undecidability results. Observe that they solve in particular the open problems we speak of in our introduction.

COROLLARY 4.3 : Let A be an alphabet with at least two letters. Then the equality problem, the inequality problem, the local equality problem and the local inequality problem are all undecidable problems for $\mathcal{M}$ or $\mathcal{N}$-rational series over A.

Note : Our undecidability result implies in particular that no "equality theorem" in the sense of Eilenberg (cf [6] th. VI.8.1) can hold in $\mathcal{M}$. However it is interesting to notice that this can also be directly proved. Indeed, if we consider the following family of matrices

$$M_n = \begin{pmatrix} 1 & n \\ 1 & 0 \end{pmatrix}$$

which is indexed by $n \in \mathbb{N}$, it is easy to prove that we have

$$S_n = \sum_{k=0}^{+\infty} (M_n)_{1,1}^k \, a^k = \sum_{k=0}^{n} k \, a^k + \sum_{k=n+1}^{+\infty} (n+1) \, a^k$$

It follows from this computation that the two distinct series S_n and S_{n+1} (both associated to a $\mathcal{M}$-representation of order 2) coincide up to the order n. Hence we obtain effectively that no "equality theorem" (cf [6] th. VI.8.1) is possible for the tropical semiring, even in fact with one-letter series.

Moreover we can also obtain as an application of our methods the following decidability results which make complete our study of the decidability of the four problems considered in section 2 for $\mathcal{Z}$, $\mathcal{M}$ and $\mathcal{N}$.

COROLLARY 4.4 : The equality problem, the inequality problem, the local equality problem and the local inequality problem are decidable for $\mathcal{M}$, $\mathcal{N}$ or $\mathcal{Z}$-rational series over a *one-letter* alphabet $A = \{a\}$.

Proof : According to theorems 4.1, 4.2 and to propositions 2.1 and 2.2, it suffices to show that the local equality problem is decidable for $\mathcal{M}$-rational series over a one-letter alphabet in order to prove our corollary. Using now a classical embedding due to C. Choffrut, of $\mathcal{M}$ into the semiring $Rat(b^*)$ of rational languages over a one-letter alphabet $\{b\}$

(cf [3] or [4]), this last problem appears in fact as an intersection problem for special kinds of rational languages of $Rat(a^* \times b^*)$. The decidability of our result follows now from the decidability of the intersection problem for $Rat(a^* \times b^*)$ (see [7] for instance).

■

Note : Using a fine study of the iterated power of a square matrix with entries in $\mathcal{Z}$, it can also be shown directly that the equality problem for one-letter $\mathcal{Z}$-rational series is decidable.

Acknowledgements

I want to thank here professor I. Simon for the personal papers he communicated me and also professor S. Grigorieff who indicated me the crucial reference [5]. Finally I must also thank the "LAboratoire de Combinatoire et d'Informatique Mathématique" (LACIM; Université du Québec à Montréal) for its kind support during the preparation of the final version of this paper.

References

[1] ADLER A., *A reduction of homogeneous diophantine problems*, Journ. of London Math. Soc. (2), **3**, pp. 446-448, 1971

[2] BERSTEL J., REUTENAUER C., *Rational series and their languages*, Springer Verlag, 1986

[3] CHOFFRUT C., *Séries rationnelles d'image finie*, Technical Report 79-6, LITP, Paris, 1979

[4] CHOFFRUT C., *Rational relations and rational series*, Theor. Comput. Sci., 1992 (To appear)

[5] DAVIS M., MATIJASEVIC Y., ROBINSON J., *Hilbert's tenth problem, diophantine equations : positive aspects of a negative solution*, Proceedings of Symposia in Pure Mathematics, Vol. 28, pp. 323-378, 1976

[6] EILENBERG S., *Automata, languages and machines*, Vol. A, Academic Press, 1974

[7] GIBBONS A., RYTTER W., *On the decidability of some problems about rational subsets of free partially commutative monoids*, Theor. Comp. Sci., **48**, pp. 329-337, 1986

[8] SIMON I., *Recognizable sets with multiplicities in the tropical semiring*, [in "MFCS'88 Proceedings"], Lect. Notes in Comput. Sci., **324**, p. 107-120, Springer Verlag, 1988

[9] SIMON I., *Some open problems for automata with multiplicities*, Private communication